

AN ELEMENTAL ERDŐS–KAC THEOREM FOR ALGEBRAIC NUMBER FIELDS

PAUL POLLACK

ABSTRACT. Fix a number field K . For each nonzero $\alpha \in \mathbf{Z}_K$, let $\nu(\alpha)$ denote the number of distinct, nonassociate irreducible divisors of α . We show that $\nu(\alpha)$ is normally distributed with mean proportional to $(\log \log |N(\alpha)|)^D$ and standard deviation proportional to $(\log \log |N(\alpha)|)^{D-1/2}$. Here D , as well as the constants of proportionality, depend only on the class group of K . For example, for each fixed real λ , the proportion of $\alpha \in \mathbf{Z}[\sqrt{-5}]$ with

$$\nu(\alpha) \leq \frac{1}{8}(\log \log N(\alpha))^2 + \frac{\lambda}{2\sqrt{2}}(\log \log N(\alpha))^{3/2}$$

is given by $\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-t^2/2} dt$. As further evidence that “irreducibles play a game of chance”, we show that the values $\nu(\alpha)$ are equidistributed modulo m for every fixed m .

1. INTRODUCTION

The field of probabilistic number theory was born in 1939 out of a fruitful collaboration of Erdős and Kac. Let $\omega(n)$ denote the number of distinct prime factors of the positive integer n . The celebrated *Erdős–Kac theorem* asserts that the quantity

$$\frac{\omega(n) - \log \log x}{\sqrt{\log \log x}},$$

thought of as a random variable on the natural numbers $n \leq x$ (with the uniform measure), converges in law to a standard Gaussian, as $x \rightarrow \infty$ [EK40]. In this statement, $\log \log x$ may be changed to $\log \log n$ without affecting the meaning, since the two quantities differ by less than 1 for all $n \in (x^{1/e}, x]$. Thus, the theorem is often summarized by saying that $\omega(n)$ is normally distributed with mean $\log \log n$ and standard deviation $\sqrt{\log \log n}$.

Variants of the Erdős–Kac theorem abound (see [Kro66], [Ell80], [Liu04], [KL08], and the references in [GS07]). In this article, we describe what appears to be a new generalization in the number field setting.

Suppose that K is a number field with ring of integers \mathbf{Z}_K . Let $\text{Id}(\mathbf{Z}_K)$ denote the (commutative, cancellative) monoid of nonzero integral ideals of \mathbf{Z}_K , and let $\text{Prin}(\mathbf{Z}_K)$ denote the submonoid of principal ideals. For each $\mathfrak{a} \in \text{Id}(\mathbf{Z}_K)$, let $\omega(\mathfrak{a})$ denote the number of distinct prime ideal factors of \mathfrak{a} . In [Liu04], Liu proves an $\text{Id}(\mathbf{Z}_K)$ -generalization of Erdős–Kac, namely that $\omega(\mathfrak{a})$ is normally distributed with mean $\log \log N(\mathfrak{a})$ and standard deviation $\sqrt{\log \log N(\mathfrak{a})}$.

The “fundamental theorem of ideal theory” asserts that $\text{Id}(\mathbf{Z}_K)$ is a factorial monoid, with the prime elements in the monoid sense coinciding with the nonzero prime ideals of \mathbf{Z}_K . By contrast, $\text{Prin}(\mathbf{Z}_K)$ is in general not factorial, as shown by the famous example

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = (2)(3)$$

2000 *Mathematics Subject Classification*. 11N37. Secondary 11R27, 11R29.

Key words and phrases. Erdős–Kac theorem, Davenport constant, number field, irreducible element.

when $K = \mathbf{Q}(\sqrt{-5})$. Notwithstanding the failure of unique factorization, it is still sensible to count the number of irreducible divisors of an element of $\text{Prin}(\mathbf{Z}_K)$ and to ask if something like the Erdős–Kac theorem holds. Our main theorem asserts that this is indeed the case.

For each nonzero $\alpha \in \mathbf{Z}_K$, we let $\nu(\alpha)$ denote the number of nonassociate irreducible divisors of α . (Equivalently, $\nu(\alpha)$ is the number of irreducible divisors of (α) in the monoid $\text{Prin}(\mathbf{Z}_K)$.) We let \log_k denote the k -fold iterated logarithm.

Theorem 1. *Let K be a number field. There are positive constants A and B , as well as a positive integer D , such that the following holds. For each fixed $\lambda > 0$,*

$$\frac{\#\{(\alpha) : 0 < |N(\alpha)| \leq x \text{ and } \nu(\alpha) \leq A(\log_2 x)^D + \lambda \cdot B(\log_2 x)^{D-\frac{1}{2}}\}}{\#\{(\alpha) : 0 < |N(\alpha)| \leq x\}} \rightarrow \int_{-\infty}^{\lambda} e^{-t^2/2} dt,$$

as $x \rightarrow \infty$. Moreover, the constants A , B , and D depend only on the isomorphism type of the class group of K .

We can summarize Theorem 1 as asserting that $\nu(\alpha)$ has a normal distribution with mean $A(\log_2 |N(\alpha)|)^D$ and standard deviation $B(\log_2 |N(\alpha)|)^{D-\frac{1}{2}}$.

We say a little about the values of A , B , and D . Of the three, D is the simplest to describe: It is the smallest integer with the property that any sequence of D elements of the class group $\text{Cl}(\mathbf{Z}_K)$ contains a nonempty subsequence which multiplies to the identity. (If G is any finite abelian group, the analogous quantity has become known as the *Davenport constant* of G , and there is now a large literature on determining values of Davenport constants.) The appearance of D in Theorem 1 is not so surprising. In fact, the constant D is important to us for precisely the same reason it first caught the attention of Davenport: D is the maximal number of prime ideals (counting multiplicity) that appear in the decomposition of an irreducible element of \mathbf{Z}_K .¹ The constants A and B are more complicated to define, but in the case when $\text{Cl}(\mathbf{Z}_K)$ is cyclic of order h , we will show that $A = \phi(h)h^{-h}h!^{-1}$ and $B = h^{-h+3/2}h!^{-1}\phi(h)^{1/2}$.

A few words about strategy are in order. The function $\nu(\alpha)$ is not additive in any reasonable sense; even if α and β generate comaximal ideals of \mathbf{Z}_K , we need not have $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$. For example, in $\mathbf{Z}[\sqrt{-5}]$, we have $\nu(2) = 1$ and $\nu(3) = 1$, whereas $\nu(6) = 4$. To work around this, we cook up an additive function f on $\text{Id}(\mathbf{Z}_K)$ such that the behavior of ν is — most of the time, and on the scale important for us — determined by the distribution of f restricted to $\text{Prin}(\mathbf{Z}_K)$. We then study the distribution of $f|_{\text{Prin}(\mathbf{Z}_K)}$ using the method of Granville–Soundararajan for proving Erdős–Kac type theorems [GS07].

Of course, many other problems concerning ν could be investigated. We content ourselves with proving one additional result further reinforcing that “irreducibles play a game of chance.”

Theorem 2. *Fix $m \in \mathbf{Z}^+$. Then $\nu(\alpha)$ is equidistributed modulo m as α ranges over \mathbf{Z}_K . More precisely, for each $a \in \mathbf{Z}$,*

$$\lim_{x \rightarrow \infty} \frac{\#\{(\alpha) : 0 < |N(\alpha)| \leq x, \nu(\alpha) \equiv a \pmod{m}\}}{\#\{(\alpha) : 0 < |N(\alpha)| \leq x\}} = \frac{1}{m}.$$

When $K = \mathbf{Q}$, this result is well-known (compare with [Sel39], [Pil40], [Add57]). In fact, when $K = \mathbf{Q}$ and $m = 2$, it goes back to von Mangoldt [Man97]; that case was later proved to be “elementarily equivalent” to the prime number theorem in work of Landau [Lan99, Lan11]. (Actually, von Mangoldt and Landau deal with squarefree positive integers, but a convolution argument shows that the equidistribution assertion for squarefree integers

¹According to Olson [Ols69], Davenport reported this observation at the Midwestern conference on group theory and number theory, Ohio State University, April 1966.

is “elementarily equivalent” to the assertion for all positive integers.) Our proof of Theorem 2 is easily adapted to prove the equidistribution mod m of the count of prime ideal divisors of elements of $\text{Id}(\mathbf{Z}_K)$ (this is again classical when $m = 2$ [Lan03]), or of $\text{Prin}(\mathbf{Z}_K)$; in fact, the arguments in these cases are much simpler.

Several further quantitative problems concerning factorizations in $\text{Prin}(\mathbf{Z}_K)$ have been considered by Geroldinger, Halter-Koch, Kaczorowski, Narkiewicz, Odoni, Rémond, Śliwa, and others. The interested reader is referred to the discussion in Chapter 9 of [Nar04] as well as the extensive end-of-chapter references there. See also [GHK06, Chapter 9].

2. ALGEBRO-ANALYTIC INPUT

For the rest of this paper, K is a degree d number field admitting r_1 real embeddings and r_2 pairs of complex conjugate embeddings, so that $d = r_1 + 2r_2$. We let $h := \#\text{Cl}(\mathbf{Z}_K)$ denote the class number, R the regulator, Δ the discriminant, and w the number of roots of unity contained in K . We fix an ordering $\mathcal{C}_1, \dots, \mathcal{C}_h$ of the elements of $\text{Cl}(\mathbf{Z}_K)$. Elements of $\text{Id}(\mathbf{Z}_K)$ are generally indicated with Fraktur letters; \mathfrak{p} and \mathfrak{q} are reserved for nonzero prime ideals of \mathbf{Z}_K . Implied constants may always depend on K without further mention.

The next two results are classical.

Lemma 3. *For each ideal class \mathcal{C} of \mathbf{Z}_K , and all $x \geq 1$,*

$$\sum_{\substack{N\mathfrak{a} \leq x \\ \mathfrak{a} \in \mathcal{C}}} 1 = \frac{\Psi x}{h} + O(x^{1-\frac{1}{d}}), \quad \text{where} \quad \Psi := \frac{2^{r_1+r_2} \pi^s R}{w \sqrt{|\Delta|}}.$$

Proof. This is due to Weber [Web96]. □

Lemma 4. *For each ideal class \mathcal{C} of \mathbf{Z}_K , and all $x \geq 3$,*

$$\sum_{\substack{N\mathfrak{p} \leq x \\ \mathfrak{p} \in \mathcal{C}}} \frac{1}{|\mathfrak{p}|} = \frac{1}{h} \log_2 x + O(1).$$

Proof. This follows from Landau’s ideal class variant of the prime ideal theorem (with error term) [Lan18, Satz LXXXV], after partial summation. □

3. REDUCTION TO A STANDARD ERDŐS-KAC PROBLEM

3.1. Preliminary anatomical results. We begin by recording two easy consequences of the analytic lemmas recalled in the preceding section. For each $i = 1, 2, \dots, h$, let $\omega_i(\mathfrak{a})$ denote the number of distinct prime ideal factors of \mathfrak{a} from \mathcal{C}_i , and let $\Omega_i(\mathfrak{a})$ denote the corresponding count with multiplicity. Then ω_i and Ω_i are additive functions on $\text{Id}(\mathbf{Z}_K)$, in the sense that $\omega_i(\mathfrak{a}\mathfrak{b}) = \omega_i(\mathfrak{a}) + \omega_i(\mathfrak{b})$ for comaximal ideals \mathfrak{a} and \mathfrak{b} , and similarly for Ω_i .

Proposition 5. *For each $i = 1, 2, \dots, h$, and all $x \geq 3$, we have*

$$\sum_{N(\mathfrak{a}) \leq x} \left(\omega_i(\mathfrak{a}) - \frac{1}{h} \log_2 x \right)^2 = O(x \log_2 x).$$

Proposition 6. *For each $i = 1, 2, \dots, h$, and all $x \geq 3$, we have*

$$\sum_{N(\mathfrak{a}) \leq x} (\Omega_i(\mathfrak{a}) - \omega_i(\mathfrak{a})) = O(x).$$

Propositions 5 and 6 follow by a straightforward imitation of the classical proofs for $K = \mathbf{Q}$ (when $h = 1$), as found in Hardy and Wright [HW08, see eqs. (22.10.1), (22.10.2), and (22.11.7)].

3.2. The *type* of an irreducible and a decomposition of $\nu(\alpha)$. Let π be an irreducible element of \mathbf{Z}_K . Suppose that the decomposition of (π) into prime ideals takes the form

$$(1) \quad (\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_g.$$

The irreducibility of π guarantees that no nonempty, proper subsequence of $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ multiplies to a principal ideal. Hence, $g \leq D$, the Davenport constant of the class group $\text{Cl}(\mathbf{Z}_K)$. On the other hand, if $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ are prime ideals whose product is principal but no nonempty proper subproduct is principal, then $\mathfrak{p}_1 \cdots \mathfrak{p}_g = (\pi)$ for an irreducible π . Since every ideal class contains prime ideals, one can construct irreducibles π with D prime ideal factors (counting multiplicity): choose $\mathfrak{p}_1, \dots, \mathfrak{p}_{D-1}$ having no nontrivial principal subproduct, and choose \mathfrak{p}_D so that $\mathfrak{p}_1 \cdots \mathfrak{p}_D$ is principal. Then each generator π of $\mathfrak{p}_1 \cdots \mathfrak{p}_D$ is irreducible. We thus recover Davenport's result that D is the maximal number of prime ideals appearing in the decomposition of an irreducible element of \mathbf{Z}_K .

Define the *type* τ of π as the integer tuple (t_1, \dots, t_h) , where t_i is the number of \mathfrak{p} in (1) belonging to \mathcal{C}_i , counted with multiplicity. Let \mathcal{T} denote the set of types τ that correspond to some irreducible. For each $\tau = (t_1, \dots, t_h) \in \mathcal{T}$, we have $t_1 + \dots + t_h = g \leq D$. When $t_1 + \dots + t_h = D$, we say τ is of *maximal length*.

For $\alpha \in \mathbf{Z}_K$ and $\tau \in \mathcal{T}$, we define $\nu_\tau(\alpha)$ as the number of distinct nonassociate irreducibles dividing α and having type τ . Thus,

$$\nu(\alpha) = \sum_{\tau \in \mathcal{T}} \nu_\tau(\alpha).$$

We now turn attention to the summands $\nu_\tau(\alpha)$.

Specifying a type- τ irreducible factor of α amounts to making h choices: For each $1 \leq i \leq h$, we must choose t_i prime ideals (not necessarily distinct) from the multiset of prime ideals dividing α_i belonging to the class \mathcal{C}_i . Abusing notation somewhat and writing $\omega_i(\alpha)$ for $\omega_i((\alpha))$, and similarly for Ω_i , the number of ways the i th choice can be made is bounded below by $\binom{\omega_i(\alpha)}{t_i}$ and bounded above by $\binom{\Omega_i(\alpha)}{t_i}$. Hence,

$$(2) \quad \prod_{i=1}^h \binom{\omega_i(\alpha)}{t_i} \leq \nu_\tau(\alpha) \leq \prod_{i=1}^h \binom{\Omega_i(\alpha)}{t_i}.$$

In order to obtain useful estimates from (2), we will assume that α avoids a small exceptional set. Let $x \geq 3$, and let α be a nonzero element of \mathbf{Z}_K with $|N(\alpha)| \leq x$. It is convenient for what follows if (α) satisfies

- (i) $|\omega_i(\alpha) - \frac{1}{h} \log_2 x| < (\log_2 x)^{2/3}$ for all $i = 1, 2, \dots, h$,
- (ii) $|\Omega_i(\alpha) - \omega_i(\alpha)| < \log_3 x$ for all $i = 1, 2, \dots, h$.

Let \mathcal{E} denote the set of principal ideals (α) of norm not exceeding x for which one at least of (i) or (ii) fails. Propositions 5 and 6 imply that

$$\#\mathcal{E} \ll x / \log_3 x.$$

In particular, \mathcal{E} makes up asymptotically 0% of the the principal ideals of norm bounded by x , as $x \rightarrow \infty$.

Suppose that $(\alpha) \notin \mathcal{E}$. Using (i), we see that

$$(3) \quad \begin{aligned} \prod_{i=1}^h \binom{\omega_i(\alpha)}{t_i} &= \prod_{i=1}^h \left(\frac{\omega_i(\alpha)^{t_i}}{t_i!} (1 + O(1/\log_2 x)) \right) \\ &= \left(\prod_{i=1}^h \frac{\omega_i(\alpha)^{t_i}}{t_i!} \right) (1 + O(1/\log_2 x)). \end{aligned}$$

On the other hand, (i) and (ii) together imply that $\Omega_i(\alpha)/\omega_i(\alpha) = 1 + O(\log_3 x / \log_2 x)$ for each $i = 1, 2, \dots, h$. Hence,

$$(4) \quad \begin{aligned} \prod_{i=1}^h \binom{\Omega_i(\alpha)}{t_i} &= \prod_{i=1}^h \left(\frac{\Omega_i(\alpha)^{t_i}}{t_i!} (1 + O(1/\log_2 x)) \right) \\ &= \left(\prod_{i=1}^h \frac{\omega_i(\alpha)^{t_i}}{t_i!} \right) (1 + O(\log_3 x / \log_2 x)). \end{aligned}$$

If τ is not of maximal length, so that $t_1 + \dots + t_h \leq D - 1$, we deduce from the upper bound in (2) along with (i) and (4) that

$$\nu_\tau(\alpha) = O((\log_2 x)^{D-1}).$$

Suppose now that τ is of maximal length. Then combining (2), (3), and (4) with (i) reveals that

$$(5) \quad \nu_\tau(\alpha) = \prod_{i=1}^h \frac{\omega_i(\alpha)^{t_i}}{t_i!} + O((\log_2 x)^{D-1} \log_3 x).$$

Write $\omega_i(\alpha) = \frac{1}{h} \log_2 x \left(1 + \frac{\omega_i(\alpha) - \frac{1}{h} \log_2 x}{\frac{1}{h} \log_2 x} \right)$. Then (keeping in mind (i))

$$\frac{\omega_i(\alpha)^{t_i}}{t_i!} = \frac{1}{t_i!} \left(\frac{1}{h} \log_2 x \right)^{t_i} \left(1 + t_i \frac{\omega_i(\alpha) - \frac{1}{h} \log_2 x}{\frac{1}{h} \log_2 x} + O((\log_2 x)^{-2/3}) \right).$$

Inserting this into (5),

$$\nu_\tau(\alpha) = \left(\prod_{i=1}^h \frac{1}{t_i!} \right) \left(\frac{1}{h} \log_2 x \right)^D \cdot \left(1 + \frac{\sum_{j=1}^h t_j \omega_j(\alpha) - \frac{D}{h} \log_2 x}{\frac{1}{h} \log_2 x} + O((\log_2 x)^{-2/3}) \right).$$

Now sum on $\tau \in \mathcal{T}$. To keep track of the components of the various τ , instead of t_1, \dots, t_h , we switch notation to $t_1(\tau), \dots, t_h(\tau)$. Then

$$(6) \quad \begin{aligned} \nu(\alpha) &= \left(\sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!} \right) \left(\frac{1}{h} \log_2 x \right)^D \\ &+ \left(\frac{1}{h} \log_2 x \right)^{D-1} \left(\sum_{j=1}^h \left(\sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} t_j(\tau) \prod_{i=1}^h \frac{1}{t_i(\tau)!} \right) \omega_j(\alpha) - \left(\frac{D}{h} \sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!} \right) \log_2 x \right) \\ &+ O((\log_2 x)^{D-2/3}). \end{aligned}$$

To continue, for $1 \leq j \leq h$, set

$$(7) \quad \kappa_j = \sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} t_j(\tau) \prod_{i=1}^h \frac{1}{t_i(\tau)!}.$$

Then

$$\sum_{j=1}^h \kappa_j = \sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!} \sum_{j=1}^h t_j(\tau) = D \sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!}.$$

In the next section, we will prove the following Erdős–Kac type result for certain additive functions f on $\text{Id}(\mathbf{Z}_K)$, restricted to $\text{Prin}(\mathbf{Z}_K)$.

Theorem 7. *Let $\kappa_1, \dots, \kappa_h$ be nonnegative constants, not all of which vanish. For nonzero $\alpha \in \mathbf{Z}_K$, let*

$$f(\alpha) = \sum_{j=1}^h \kappa_j \omega_j(\alpha).$$

As $x \rightarrow \infty$, the quantity

$$\frac{f(\alpha) - \left(\frac{1}{h} \sum_{j=1}^h \kappa_j\right) \log_2 x}{\sqrt{\left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2\right) \log_2 x}},$$

considered as a random variable on the space of nonzero principal ideals (α) of norm $\leq x$ (with the uniform measure), converges in law to a standard normal distribution.

Theorem 1 follows easily from Theorem 7. Indeed, from (6), we have that when $(\alpha) \notin \mathfrak{E}$,

$$\begin{aligned} \frac{\nu(\alpha) - \left(\sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!}\right) \left(\frac{1}{h} \log_2 x\right)^D}{\left(\frac{1}{h} \log_2 x\right)^{D-1} \sqrt{\left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2\right) \log_2 x}} \\ = \frac{\sum_{j=1}^h \kappa_j \omega_j(\alpha) - \left(\frac{1}{h} \sum_{j=1}^h \kappa_j\right) \log_2 x}{\sqrt{\left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2\right) \log_2 x}} + O((\log_2 x)^{-1/6}). \end{aligned}$$

Since only $o(x)$ ideals (α) land in \mathfrak{E} , and $(\log_2 x)^{-1/6} = o(1)$, Theorem 7 implies Theorem 1 with

$$A = \frac{1}{h^D} \sum_{\substack{\tau \in \mathcal{T} \\ \tau \text{ maximal}}} \prod_{i=1}^h \frac{1}{t_i(\tau)!} \quad \text{i.e.,} \quad A = \frac{1}{D h^D} \sum_{j=1}^h \kappa_j,$$

and

$$B = \frac{1}{h^{D-1/2}} \sqrt{\sum_{j=1}^h \kappa_j^2}.$$

Example (Calculation of A and B when the class group is cyclic; cf. [BÖRS05, §4]). Suppose that $\text{Cl}(\mathbf{Z}_K)$ is a cyclic group of order h . Then $D = h$. (See [Nar04, §9.1] for basic facts about Davenport constants.) We suppose the ideal classes are numbered so that, under a fixed isomorphism of $\text{Cl}(\mathbf{Z}_K)$ with $\mathbf{Z}/h\mathbf{Z}$, the class \mathcal{C}_i corresponds to $i \bmod h$. Then there are $\phi(h)$ types τ of maximum length, namely $(0, \dots, 0, h, 0, \dots, 0)$, where the allowed positions for ‘ h ’ are precisely the units mod h (compare with [GR09, Corollary 2.1.4, p. 24]). From (7), we see that $\kappa_j = \frac{1}{(h-1)!}$ when $\gcd(j, h) = 1$ and $\kappa_j = 0$ otherwise. After a bit of algebra, we arrive at

$$A = \frac{1}{h^h h!} \phi(h) \quad \text{and} \quad B = \frac{1}{h^h h!} (h^3 \phi(h))^{1/2},$$

as claimed in the introduction.

4. PROOF OF THEOREM 7

To prove Theorem 7, we follow very closely the approach to the Erdős–Kac theorem detailed by Granville and Soundararajan [GS07]. By the method of moments (the Fréchet–Shohat theorem), to prove Theorem 7 it is sufficient to establish the following estimates.

Proposition 8. *Let k be a fixed positive integer. Suppose that x is sufficiently large. If k is even, then*

$$\begin{aligned} \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(f(\alpha) - \left(\frac{1}{h} \sum_{j=1}^k \kappa_j \right) \log_2 x \right)^k \\ = \frac{\Psi x}{h} \cdot \frac{k!}{2^{k/2} \cdot \frac{k!}{2}} \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right)^{k/2} (\log_2 x)^{k/2} + O(x(\log_2 x)^{\frac{k-1}{2}}). \end{aligned}$$

If k is odd, then

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(f(\alpha) - \left(\frac{1}{h} \sum_{j=1}^k \kappa_j \right) \log_2 x \right)^k = O((\log_2 x)^{\frac{k-1}{2}}).$$

Here the implied constants may depend not only on K but also on k and the κ_j .

Proposition 8 will be deduced from the following technical lemma. For a nonzero prime ideal \mathfrak{p} of \mathbf{Z}_K , we set $\kappa_{\mathfrak{p}} = \kappa_j$, where j is that index for which $\mathfrak{p} \in \mathcal{C}_j$.

Lemma 9. *For each nonzero prime ideal \mathfrak{p} of \mathbf{Z}_K , and each nonzero ideal \mathfrak{a} of \mathbf{Z}_K , set*

$$g_{\mathfrak{p}}(\mathfrak{a}) = \begin{cases} 1 - \frac{1}{N\mathfrak{p}} & \text{if } \mathfrak{p} \mid \mathfrak{a}, \\ -\frac{1}{N\mathfrak{p}} & \text{if } \mathfrak{p} \nmid \mathfrak{a}. \end{cases}$$

Fix a positive integer k . Suppose x is sufficiently large, and let $z = x^{\frac{1}{2dk}}$. If k is even, then

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(\sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) \right)^k = \frac{\Psi x}{h} \cdot \frac{k!}{2^{k/2} \cdot \frac{k!}{2}} \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right)^{k/2} (\log_2 x)^{k/2} + O(x(\log_2 x)^{\frac{k-1}{2}}).$$

If k is odd, then

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(\sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) \right)^k = O((\log_2 x)^{\frac{k-1}{2}}).$$

Here the implied constants may depend on K , k , and the κ_j .

Deduction of Proposition 8 from Lemma 9. For each j , let $\omega_j(\alpha; z)$ denote the number of prime ideal factors \mathfrak{p} of (α) with $\mathfrak{p} \in \mathcal{C}_j$ and $N\mathfrak{p} \leq z$. Using Lemma 4, we see that

$$\begin{aligned} \sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) &= \sum_{\substack{\mathfrak{p} \mid \alpha \\ N\mathfrak{p} \leq z}} \kappa_{\mathfrak{p}} - \sum_{N\mathfrak{p} \leq z} \frac{\kappa_{\mathfrak{p}}}{N\mathfrak{p}} = \sum_{j=1}^h \kappa_j \omega_j(\alpha; z) - \sum_{j=1}^h \kappa_j \left(\frac{1}{h} \log_2 z + O(1) \right) \\ &= f(\alpha) - \left(\frac{1}{h} \sum_{j=1}^h \kappa_j \right) \log_2 x + O(1). \end{aligned}$$

To go from the first line to the second, we used that $\log_2 z = \log_2 x + O(1)$ and that (α) can have only $O(1)$ prime ideal factors of norm exceeding z . We deduce that

$$\left(f(\alpha) - \left(\frac{1}{h} \sum_{j=1}^h \kappa_j \right) \log_2 x \right)^k = \left(\sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) \right)^k + O \left(\sum_{\ell=0}^{k-1} \left| \sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) \right|^\ell \right).$$

Sum both sides over principal ideals (α) with $0 < |N(\alpha)| \leq x$. To estimate the main term on the right-hand side, we may appeal to Lemma 9. We can also use Lemma 9 to see that the even values of ℓ make an acceptable contribution to the error term. If ℓ is odd, we use Cauchy–Schwarz to deduce that

$$\begin{aligned} & \sum_{(\alpha): 0 < |N(\alpha)| \leq x} \left| \sum_{N\mathfrak{p} \leq z} \kappa_p g_{\mathfrak{p}}(\alpha) \right|^\ell \\ & \leq \left(\sum_{(\alpha): 0 < |N(\alpha)| \leq x} \left| \sum_{N\mathfrak{p} \leq z} \kappa_p g_{\mathfrak{p}}(\alpha) \right|^{\ell-1} \right)^{1/2} \left(\sum_{(\alpha): 0 < |N(\alpha)| \leq x} \left| \sum_{N\mathfrak{p} \leq z} \kappa_p g_{\mathfrak{p}}(\alpha) \right|^{\ell+1} \right)^{1/2}. \end{aligned}$$

Appealing once more to Lemma 9, we find that the contribution of the odd ℓ also fits within the O -term claimed in Proposition 8. \square

Proof of Lemma 9. If $\mathfrak{r} = \prod_i \mathfrak{p}_i^{e_i}$, put $g_{\mathfrak{r}}(\mathfrak{a}) = \prod_i g_{\mathfrak{p}}(\mathfrak{a})^{e_i}$. Then

$$(8) \quad \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(\sum_{N\mathfrak{p} \leq z} \kappa_p g_{\mathfrak{p}}(\alpha) \right)^k = \sum_{\substack{\mathfrak{p}_1, \dots, \mathfrak{p}_k \\ \text{each } N\mathfrak{p}_i \leq z}} \kappa_{\mathfrak{p}_1} \cdots \kappa_{\mathfrak{p}_k} \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} g_{\mathfrak{p}_1 \cdots \mathfrak{p}_k}(\alpha).$$

To proceed, we consider more generally sums of the form

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} g_{\mathfrak{r}}(\alpha),$$

for any \mathfrak{r} with $N\mathfrak{r} \leq z^k$. Write $\mathfrak{r} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}$, where the \mathfrak{q}_i are distinct prime ideals. Put $\mathfrak{R} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. If $\mathfrak{d} = \gcd((\alpha), \mathfrak{R})$, then $g_{\mathfrak{r}}(\alpha) = g_{\mathfrak{r}}(\mathfrak{d})$. Hence,

$$(9) \quad \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} g_{\mathfrak{r}}(\alpha) = \sum_{\mathfrak{d} | \mathfrak{R}} g_{\mathfrak{r}}(\mathfrak{d}) \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x \\ \gcd((\alpha), \mathfrak{R}) = \mathfrak{d}}} 1.$$

We turn attention to the right-hand inner sum. Observe that $\gcd((\alpha), \mathfrak{R}) = \mathfrak{d}$ precisely when $\mathfrak{d} \mid \alpha$ and $\alpha\mathfrak{d}^{-1}$ and $\mathfrak{R}\mathfrak{d}^{-1}$ are coprime. Thus, thinking of $\mathfrak{b} = \alpha\mathfrak{d}^{-1}$, the inner sum equals

$$\sum_{\substack{\mathfrak{b}: N\mathfrak{b} \leq x/N\mathfrak{d} \\ [\mathfrak{b}] = [\mathfrak{d}]^{-1} \\ \gcd(\mathfrak{b}, \mathfrak{R}\mathfrak{d}^{-1}) = 1}} 1.$$

(Here and below, $[\cdot]$ denotes the image of an ideal in the class group $\text{Cl}(\mathbf{Z}_K)$.) Letting μ denote the Möbius function on $\text{Id}(\mathbf{Z}_K)$,

$$\sum_{\substack{\mathfrak{b}: N\mathfrak{b} \leq x/N\mathfrak{d} \\ [\mathfrak{b}] = [\mathfrak{d}]^{-1} \\ \gcd(\mathfrak{b}, \mathfrak{R}\mathfrak{d}^{-1}) = 1}} 1 = \sum_{\substack{\mathfrak{b}: N\mathfrak{b} \leq x/N\mathfrak{d} \\ [\mathfrak{b}] = [\mathfrak{d}]^{-1}}} \sum_{\substack{\mathfrak{e} | \mathfrak{R}\mathfrak{d}^{-1} \\ \mathfrak{e} | \mathfrak{b}}} \mu(\mathfrak{e}) = \sum_{\mathfrak{e} | \mathfrak{R}\mathfrak{d}^{-1}} \mu(\mathfrak{e}) \sum_{\substack{\mathfrak{b}: N\mathfrak{b} \leq x/N\mathfrak{d} \\ [\mathfrak{b}] = [\mathfrak{d}]^{-1} \\ \mathfrak{e} | \mathfrak{b}}} 1.$$

Writing $\mathfrak{b} = \mathfrak{c}\mathfrak{f}$, we see that

$$\begin{aligned} \sum_{\mathfrak{c}|\mathfrak{R}\mathfrak{d}^{-1}} \mu(\mathfrak{c}) \sum_{\substack{\mathfrak{b}: N\mathfrak{b} \leq x/N\mathfrak{d} \\ [\mathfrak{b}] = [\mathfrak{d}]^{-1} \\ \mathfrak{c}|\mathfrak{b}}} 1 &= \sum_{\mathfrak{c}|\mathfrak{R}\mathfrak{d}^{-1}} \mu(\mathfrak{c}) \sum_{\substack{\mathfrak{f}: N\mathfrak{f} \leq x/N(\mathfrak{d}\mathfrak{c}) \\ [\mathfrak{f}] = [\mathfrak{d}\mathfrak{c}]^{-1}}} 1 \\ &= \sum_{\mathfrak{c}|\mathfrak{R}\mathfrak{d}^{-1}} \left(\frac{\Psi x}{h} \frac{\mu(\mathfrak{c})}{N\mathfrak{d}N\mathfrak{c}} + O\left(\left(\frac{x}{N(\mathfrak{d}\mathfrak{c})}\right)^{1-1/d}\right) \right) \\ &= \frac{\Psi x}{h \cdot N\mathfrak{d}} \cdot \frac{\phi(\mathfrak{R}\mathfrak{d}^{-1})}{N(\mathfrak{R}\mathfrak{d}^{-1})} + O\left(x^{1-1/d} \sum_{\mathfrak{c}|\mathfrak{R}\mathfrak{d}^{-1}} \frac{1}{(N(\mathfrak{d}\mathfrak{c}))^{1-1/d}}\right). \end{aligned}$$

(Here the ideal-theoretic ϕ -function is defined by $\phi(\mathfrak{u}) = \#(\mathfrak{O}/\mathfrak{u})^\times$.) Plugging this back into (9), and using that $|g_{\mathfrak{r}}(\mathfrak{d})| \leq 1$,

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} g_{\mathfrak{r}}(\alpha) = \frac{\Psi x}{h} \cdot \frac{1}{N\mathfrak{R}} \sum_{\mathfrak{d}|\mathfrak{R}} g_{\mathfrak{r}}(\mathfrak{d}) \phi(\mathfrak{R}\mathfrak{d}^{-1}) + O\left(x^{1-1/d} \sum_{\substack{\mathfrak{d}, \mathfrak{c} \\ \mathfrak{d}\mathfrak{c}|\mathfrak{R}}} \frac{1}{N(\mathfrak{d}\mathfrak{c})^{1-1/d}}\right).$$

The error term here is harmless: For any $\epsilon > 0$, there are $\ll_{\epsilon} N(\mathfrak{R})^{\epsilon} \leq z^{k\epsilon} = x^{\epsilon/2d}$ ideal divisors of \mathfrak{R} . Hence, the number of pairs $\mathfrak{d}, \mathfrak{c}$ with $\mathfrak{d}\mathfrak{c}$ dividing \mathfrak{R} is crudely $\ll_{\epsilon} x^{\epsilon/d}$. Trivially, $1/N(\mathfrak{d}\mathfrak{c})^{1-1/d} \leq 1$, and so we see (taking $\epsilon = 1/4$) that the O -term above is $O(x^{1-\frac{3}{4d}})$. The sum on \mathfrak{d} dividing \mathfrak{R} appearing in the main term can be explicitly evaluated; we find that

$$(10) \quad \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} g_{\mathfrak{r}}(\alpha) = \frac{\Psi x}{h} \cdot G(\mathfrak{r}) + O(x^{1-\frac{3}{4d}}),$$

where

$$G(\mathfrak{r}) := \prod_{\mathfrak{q}^e \parallel \mathfrak{r}} \left(\frac{1}{N\mathfrak{q}} \left(1 - \frac{1}{N\mathfrak{q}}\right)^e + \left(\frac{-1}{N\mathfrak{q}}\right)^e \left(1 - \frac{1}{N\mathfrak{q}}\right) \right).$$

We see from this formula that $G(\mathfrak{r})$ vanishes unless \mathfrak{r} is squarefull, by which we mean that each prime ideal divisor of \mathfrak{r} is repeated.

Substituting (10) back into (8),

$$\sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \left(\sum_{N\mathfrak{p} \leq z} \kappa_{\mathfrak{p}} g_{\mathfrak{p}}(\alpha) \right)^k = \frac{\Psi x}{h} \sum_{\substack{\mathfrak{p}_1, \dots, \mathfrak{p}_k \\ \text{each } N\mathfrak{p}_i \leq z \\ \mathfrak{p}_1 \cdots \mathfrak{p}_k \text{ squarefull}}} \kappa_{\mathfrak{p}_1} \cdots \kappa_{\mathfrak{p}_k} G(\mathfrak{p}_1 \cdots \mathfrak{p}_k) + O(x^{1-\frac{3}{4d}} z^k).$$

The O -term is $\ll x^{1-\frac{1}{4d}}$, which will be negligible for us. The main term can be rewritten as

$$\frac{\Psi x}{h} \sum_{s \leq k/2} \frac{1}{s!} \sum_{\substack{\mathfrak{q}_1, \dots, \mathfrak{q}_s \\ \mathfrak{q}_i \text{ distinct} \\ \text{each } N\mathfrak{q}_i \leq z}} \sum_{\substack{e_1, \dots, e_s \geq 2 \\ \sum e_i = k}} \frac{k!}{e_1! \cdots e_s!} \cdot \kappa_{\mathfrak{q}_1}^{e_1} \cdots \kappa_{\mathfrak{q}_s}^{e_s} \cdot G(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}).$$

Let us estimate the contribution from the values of $s < k/2$. We use the easily seen inequality $|G(\mathbf{q}_1^{e_1} \cdots \mathbf{q}_s^{e_s})| \leq \frac{1}{N(\mathbf{q}_1 \cdots \mathbf{q}_s)}$ to deduce that

$$\begin{aligned} \frac{\Psi x}{h} \sum_{s < k/2} \frac{1}{s!} \sum_{\substack{\mathbf{q}_1, \dots, \mathbf{q}_s \\ \mathbf{q}_i \text{ distinct} \\ \text{each } N\mathbf{q}_i \leq z}} \sum_{\substack{e_1, \dots, e_s \geq 2 \\ \sum e_i = k}} \frac{k!}{e_1! \cdots e_s!} \cdot \kappa_{\mathbf{q}_1}^{e_1} \cdots \kappa_{\mathbf{q}_s}^{e_s} \cdot G(\mathbf{q}_1^{e_1} \cdots \mathbf{q}_s^{e_s}) \\ \ll x \sum_{s < k/2} \sum_{\substack{\mathbf{q}_1, \dots, \mathbf{q}_s \\ \text{each } N\mathbf{q}_i \leq z}} \frac{1}{N(\mathbf{q}_1 \cdots \mathbf{q}_s)} = x \sum_{s < k/2} \left(\sum_{N\mathbf{q} \leq z} \frac{1}{N\mathbf{q}} \right)^s \ll x(\log_2 x)^{\lfloor (k-1)/2 \rfloor}, \end{aligned}$$

since each s in the sum is at most $\frac{k-1}{2}$ and $\sum_{N\mathbf{q} \leq z} \frac{1}{N\mathbf{q}} \leq \log_2 x + O(1)$. Thus, the values $s < k/2$ contribute $\ll x(\log_2 x)^{\frac{k-1}{2}}$ when k is odd and $\ll x(\log_2 x)^{\frac{k}{2}-1}$ when k is even. This completes the proof of Lemma 9 in the odd k case.

When k is even, there is an additional contribution corresponding to $s = k/2$ and $e_1 = e_2 = \cdots = e_{k/2} = 2$, of size

$$\frac{\Psi x}{h} \cdot \frac{k!}{2^{k/2} \cdot \frac{k!}{2!}} \sum_{\substack{\mathbf{q}_1, \dots, \mathbf{q}_{k/2} \\ \mathbf{q}_i \text{ distinct} \\ \text{each } N\mathbf{q}_i \leq z}} \prod_{i=1}^{k/2} \frac{\kappa_{\mathbf{q}_i}^2}{N\mathbf{q}_i} \left(1 - \frac{1}{N\mathbf{q}_i} \right).$$

Forgetting the distinctness restriction, we obtain an upper bound on this last sum of

$$\begin{aligned} \left(\sum_{N\mathbf{q} \leq z} \frac{\kappa_{\mathbf{q}}^2}{N\mathbf{q}} \right)^{k/2} &= \left(\sum_{j=1}^h \kappa_j^2 \sum_{\substack{N\mathbf{q} \leq z \\ \mathbf{q} \in \mathcal{C}_j}} \frac{1}{N\mathbf{q}} \right)^{k/2} \leq \left(\left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right) \log_2 x + O(1) \right)^{k/2} \\ &= \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right)^{k/2} (\log_2 x)^{k/2} + O((\log_2 x)^{\frac{k}{2}-1}). \end{aligned}$$

It is easy to obtain a lower bound of the same form. Indeed, for any given choices of $\mathbf{q}_1, \dots, \mathbf{q}_{\frac{k}{2}-1}$,

$$\begin{aligned} \sum_{\substack{N\mathbf{q} \leq z \\ \mathbf{q} \neq \mathbf{q}_1, \dots, \mathbf{q}_{\frac{k}{2}-1}}} \frac{\kappa_{\mathbf{q}}^2}{N\mathbf{q}} \left(1 - \frac{1}{N\mathbf{q}} \right) &\geq \sum_{N\mathbf{q} \leq z} \frac{\kappa_{\mathbf{q}}^2}{N\mathbf{q}} + O(1) = \sum_{j=1}^h \kappa_j^2 \sum_{\substack{N\mathbf{q} \leq z \\ \mathbf{q} \in \mathcal{C}_j}} \frac{1}{N\mathbf{q}} + O(1) \\ &= \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right) \log_2 z + O(1) = \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right) \log_2 x + O(1). \end{aligned}$$

Repeating this procedure, we eventually find that

$$\begin{aligned} \sum_{\substack{\mathbf{q}_1, \dots, \mathbf{q}_{k/2} \\ \mathbf{q}_i \text{ distinct} \\ \text{each } N\mathbf{q}_i \leq z}} \prod_{i=1}^{k/2} \frac{\kappa_{\mathbf{q}_i}^2}{N\mathbf{q}_i} \left(1 - \frac{1}{N\mathbf{q}_i} \right) &\geq \left(\left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right) \log_2 x + O(1) \right)^{k/2} \\ &= \left(\frac{1}{h} \sum_{j=1}^h \kappa_j^2 \right)^{k/2} (\log_2 x)^{k/2} + O((\log_2 x)^{\frac{k}{2}-1}). \end{aligned}$$

Combining these estimates with the results of the preceding paragraph completes the proof in the even k case. \square

Remark. Theorem 7 could also be proved by applying the results of [Kro66, Chapter 2], with Lemma 4 used as the analytic input. De Kroon proves an Erdős–Kac theorem for $f|_{\text{Prin}(\mathbf{Z}_K)}$, for additive functions f on $\text{Id}(\mathbf{Z}_K)$ satisfying conditions analogous to those in the main theorem of [EK40]. De Kroon’s approach follows [EK40], in that the central limit theorem is used in combination with Brun’s sieve. We have preferred to give a more self-contained proof illustrating the flexibility of the method of [GS07].

5. REMARKS ON THEOREM 1

5.1. A $\text{Prin}(\mathbf{Z}_K)$ -analogue of an observation of Kac. Let $d(n)$ denote the classical divisor function. In 1941, Kac [Kac41] showed that $\frac{\log d(n)}{\log 2}$ is normally distributed with mean and variance $\log_2 n$. This can be proved by the following simple argument: According to [EK40], both $\omega(n)$ and $\Omega(n)$ are normally distributed with mean and variance $\log_2 n$; now observe that $2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)}$ for all n .

Substituting the results of [Liu04] for those of [EK40], an identical argument shows that the divisor function on $\text{Id}(\mathbf{Z}_K)$ — which by abuse of notation we will also denote d — is normally distributed with mean and variance $\log_2 N(\mathfrak{a})$. Seeking a $\text{Prin}(\mathbf{Z}_K)$ analogue, define $\delta(\alpha)$ for nonzero $\alpha \in \mathbf{Z}_K$ as the number of nonassociate divisors of α . It turns out that δ is distributed in the same way as d , by which we mean that $\frac{\log \delta(\alpha)}{\log 2}$ is normal with mean and variance $\log_2 |N(\alpha)|$.

Let us sketch the proof. First, one shows that $\omega(\alpha) := \sum_{i=1}^h \omega_i(\alpha)$ and $\Omega(\alpha) := \sum_{i=1}^h \Omega_i(\alpha)$ are both normally distributed with mean and variance $\log_2 |N(\alpha)|$. For ω , this follows from Theorem 7 with $\kappa_1 = \dots = \kappa_h = 1$. The Ω assertion then follows from Proposition 6. (For these claims, one could also appeal to [Kro66].) Next, one observes that $\delta(\alpha) \leq d(\alpha) \leq 2^{\Omega(\alpha)}$. On the other hand, one can construct many nonassociate divisors of α by the following recipe: For each $i = 1, 2, \dots, h$, list the distinct prime ideal divisors of α belonging to \mathfrak{C}_i , choose a subset of these whose cardinality is a multiple of h , and then multiply the prime ideals from each of these subsets. This construction yields

$$\delta(\alpha) \geq \prod_{i=1}^h \left(\sum_{\substack{0 \leq j \leq \omega_i(\alpha) \\ h|j}} \binom{\omega_i(\alpha)}{j} \right).$$

For each i , the sum on j is $\gg 2^{\omega_i(\alpha)}$. (One can see this by rewriting the sum as $\frac{1}{h} \sum_{\zeta} (1+\zeta)^{\omega_i(\alpha)}$, where ζ runs over the h th roots of unity, and noting that $\zeta = 1$ dominates.) It follows that

$$\delta(\alpha) \gg 2^{\omega_1(\alpha) + \dots + \omega_h(\alpha)} = 2^{\omega(\alpha)}.$$

Thus,

$$2^{\omega(\alpha) + O(1)} \leq \delta(\alpha) \leq 2^{\Omega(\alpha)},$$

and now we can obtain the normal distribution result for δ in the same way as for d .

5.2. Average order results. One can show that as $x \rightarrow \infty$, the average of $\nu(\alpha)$ on principal ideals (α) of norm $\leq x$ is $\sim A(\log \log x)^D$ (for the same constant A from Theorem 1), while the corresponding average of $\delta(\alpha)$ is $\sim \frac{\Psi}{h} \log x$. These estimates are considerably simpler to prove than the normal order results discussed above. Indeed, they follow more or less immediately from

$$\sum_{\substack{(\pi): |N(\pi)| \leq x \\ \pi \text{ irreducible}}} \frac{1}{|N(\pi)|} \sim A(\log \log x)^D \quad \text{and} \quad \sum_{(\alpha): 0 < |N(\alpha)| \leq x} \frac{1}{|N(\alpha)|} \sim \frac{\Psi}{h} \log x.$$

The second of these may be derived quickly by partial summation from Lemma 3. The first can be proved by methods discussed earlier in this article, or by partial summation in conjunction with Rémond's asymptotic formula for the count of nonassociate irreducibles of bounded norm [Rém66, Théorème II, pp. 391–392, and Corollaire, pp. 409–410].

6. EQUIDISTRIBUTION OF $\nu(\alpha)$ IN RESIDUE CLASSES: PROOF OF THEOREM 2

Below, we say a multiplicative function f on $\text{Id}(\mathbf{Z}_K)$ is of *finite order* if for some positive integer r , all of the nonzero values of f are r th roots of unity.

Lemma 10. *Let f be a multiplicative function on $\text{Id}(\mathbf{Z}_K)$ of finite order. Suppose that*

$$(11) \quad \sum_{f(\mathfrak{p}) \neq 1} \frac{1}{N\mathfrak{p}} \quad \text{diverges.}$$

Then f has mean value 0 on $\text{Id}(\mathbf{Z}_K)$, in the sense that

$$\sum_{N\mathfrak{a} \leq x} f(\mathfrak{a}) = o(x),$$

as $x \rightarrow \infty$.

Proof. This appears to be well-known when $K = \mathbf{Q}$, and the argument in the general case is the same; for lack of a suitable reference we sketch the proof. We use a theorem of Halász [Hal68], as generalized to “arithmetic semigroups” (a setting which includes $\text{Id}(\mathbf{Z}_K)$) by Lucht and Reifenrath [LR01, Theorem 6.1]. It suffices to show that for each real number t , the series

$$(12) \quad \sum_{\mathfrak{p}} \frac{1 - \Re(f(\mathfrak{p}) \cdot N(\mathfrak{p})^{-it})}{N\mathfrak{p}}$$

diverges. The divergence when $t = 0$ follows quickly from (11). Now suppose that $t \neq 0$. Fix a positive integer r such that $f(\text{Id}(\mathbf{Z}_K))$ is contained in $\{0\} \cup \{\zeta : \zeta^r = 1\}$. The prime ideal theorem implies that for $\gg_r x / \log x$ prime ideals of norm not exceeding x , the quantity $N(\mathfrak{p})^{it}$ lies at a distance $\gg_r 1$ from each r th root of unity; the divergence of (12) is an easy consequence. \square

Lemma 11. *Let f be a multiplicative function on $\text{Id}(\mathbf{Z}_K)$ of finite order. Suppose that*

$$\sum_{\substack{\mathfrak{p} \text{ principal} \\ f(\mathfrak{p}) \neq 1}} \frac{1}{N\mathfrak{p}} \quad \text{diverges.}$$

Then f has mean value 0 along each ideal class, in the sense that for each $i = 1, 2, \dots, h$,

$$\sum_{\substack{N\mathfrak{a} \leq x \\ \mathfrak{a} \in \mathcal{C}_i}} f(\mathfrak{a}) = o(x),$$

as $x \rightarrow \infty$.

Proof. By the orthogonality relations for group characters, it suffices to show that for each character χ of the class group $\text{Cl}(\mathbf{Z}_K)$, the function χf has mean value 0 on $\text{Id}(\mathbf{Z}_K)$. This follows immediately from Lemma 10. \square

Proof of Theorem 2. Throughout this proof, we assume that the ideal classes \mathcal{C}_i are numbered so that \mathcal{C}_1 is the principal class. By the orthogonality relations for additive characters mod m , it suffices to show that for all nontrivial m th roots of unity ζ ,

$$(13) \quad \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x}} \zeta^{\nu(\alpha)} = o(x), \quad \text{as } x \rightarrow \infty.$$

Fix a nonzero, squarefull ideal \mathfrak{s} of \mathbf{Z}_K . We study the contribution to (13) from (α) with squarefull part \mathfrak{s} in $\text{Id}(\mathbf{Z}_K)$. Write $(\alpha) = \mathfrak{s}\mathfrak{u}$, so that \mathfrak{u} is a squarefree ideal, \mathfrak{s} and \mathfrak{u} are comaximal, and $[\mathfrak{u}] = [\mathfrak{s}]^{-1}$. Then

$$(14) \quad \nu(\alpha) = \sum_{\tau \in \mathcal{T}} \nu_\tau(\alpha) = \omega_1(\alpha) + \sum_{\substack{\tau \in \mathcal{T} \\ t_1(\tau)=0}} \nu_\tau(\alpha),$$

and

$$\omega_1(\alpha) = \omega_1(\mathfrak{s}) + \omega_1(\mathfrak{u}).$$

(We used here that $(1, 0, \dots, 0)$ is the only type in \mathcal{T} with a nonvanishing t_1 coefficient, and that $\nu_{(1,0,\dots,0)}(\alpha) = \omega_1(\alpha)$.) For each $\tau \in \mathcal{T}$ with $t_1(\tau) = 0$, let

$$\mathcal{D}(\mathfrak{s}, \tau) = \{\mathfrak{d} \in \text{Id}(\mathbf{Z}_K) : \mathfrak{d} \mid \mathfrak{s}, \Omega_i(\mathfrak{d}) \leq t_i(\tau) \text{ for all } i = 1, 2, \dots, h\}.$$

Any irreducible of type τ dividing α can be written uniquely as the product of an element of $\mathcal{D}(\mathfrak{s}, \tau)$ and a cofactor relatively prime to \mathfrak{s} . Thus,

$$(15) \quad \nu_\tau(\alpha) = \sum_{\mathfrak{d} \in \mathcal{D}(\mathfrak{s}, \tau)} \prod_{i=1}^h \binom{\Omega_i(\alpha) - \Omega_i(\mathfrak{s})}{t_i(\tau) - \Omega_i(\mathfrak{d})} = \sum_{\mathfrak{d} \in \mathcal{D}(\mathfrak{s}, \tau)} \prod_{i=2}^h \binom{\omega_i(\mathfrak{u})}{t_i(\tau) - \Omega_i(\mathfrak{d})}.$$

Keeping in mind the universal bound $t_i(\tau) \leq h$, it follows from (15) that the residue class mod m of

$$\sum_{\substack{\tau \in \mathcal{T} \\ t_1(\tau)=0}} \nu_\tau(\alpha)$$

depends only on the vector

$$(\omega_2(\mathfrak{u}) \bmod mh!, \dots, \omega_h(\mathfrak{u}) \bmod mh!) \in (\mathbf{Z}/mh!\mathbf{Z})^{h-1}.$$

Consequently, finite Fourier theory implies that

$$\zeta^{\sum_{\tau \in \mathcal{T}, t_1(\tau)=0} \nu_\tau(\alpha)}$$

can be written as a finite \mathbf{C} -linear combination of terms of the form

$$\zeta_2^{\omega_2(\mathfrak{u})} \dots \zeta_h^{\omega_h(\mathfrak{u})},$$

where ζ_2, \dots, ζ_h are $(mh!)$ th roots of unity. Referring back to (14), we see that $\zeta^{\nu(\alpha)}$ is a finite \mathbf{C} -linear combination of expressions of the form

$$\zeta^{\omega_1(\mathfrak{u})} \zeta_2^{\omega_2(\mathfrak{u})} \dots \zeta_h^{\omega_h(\mathfrak{u})}.$$

Thus,

$$\sum_{\substack{(\alpha) \\ \text{squarefull part } \mathfrak{s} \\ 0 < |N(\alpha)| \leq x}} \zeta^{\nu(\alpha)}$$

is a finite \mathbf{C} -linear combination of sums of the form

$$\sum_{\substack{N\mathfrak{u} \leq x/N(\mathfrak{s}) \\ [\mathfrak{u}] = [\mathfrak{s}]^{-1}}} \mathbf{1}_{\gcd(\mathfrak{u}, \mathfrak{s})=1} \cdot \mu^2(\mathfrak{u}) \cdot \zeta^{\omega_1(\mathfrak{u})} \zeta_2^{\omega_2(\mathfrak{u})} \dots \zeta_h^{\omega_h(\mathfrak{u})}.$$

For all choices of $(mh)!$ th roots of unity ζ_2, \dots, ζ_h , the function

$$\mathbf{u} \mapsto \mathbf{1}_{\gcd(\mathbf{u}, \mathfrak{s})=1} \cdot \mu^2(\mathbf{u}) \cdot \zeta^{\omega_1(\mathbf{u})} \zeta_2^{\omega_2(\mathbf{u})} \cdots \zeta_h^{\omega_h(\mathbf{u})}$$

satisfies the conditions of Lemma 11. Hence, the contribution to (13) from (α) with a fixed squarefull part is $o(x)$, as $x \rightarrow \infty$.

We now finish the proof of Theorem 2. Let $\epsilon > 0$. Let B be a large, fixed real number. Continuing to use \mathfrak{s} for the squarefull part of (α) , we see that the contribution to (13) from (α) with $N\mathfrak{s} \leq B$ is $o(x)$, as $x \rightarrow \infty$. On the other hand,

$$\left| \sum_{\substack{(\alpha) \\ 0 < |N(\alpha)| \leq x \\ N\mathfrak{s} > B}} \zeta^{\nu(\alpha)} \right| \leq \sum_{\substack{\mathfrak{s} \text{ squarefull} \\ B < N\mathfrak{s} \leq x}} \sum_{\substack{Na \leq x \\ \mathfrak{s} | a}} 1 \ll x \sum_{\substack{\mathfrak{s} \text{ squarefull} \\ N\mathfrak{s} > B}} \frac{1}{N\mathfrak{s}}.$$

The sum appearing here is the tail of a convergent series, since

$$\sum_{\mathfrak{s} \text{ squarefull}} \frac{1}{N\mathfrak{s}} = \prod_{\mathfrak{p}} \left(1 + \frac{1}{N\mathfrak{p}^2} + \frac{1}{N\mathfrak{p}^3} + \dots \right) < \infty.$$

So if we choose B sufficiently large, those (α) with $N\mathfrak{s} > B$ contribute less than ϵx . Since $\epsilon > 0$ is arbitrary, Theorem 2 follows. \square

Remark. The distribution of $\delta(\alpha)$ in residue classes is much more complicated than that of $\nu(\alpha)$, even in the case $K = \mathbf{Q}$ (for which see [Nar86, Chapter 5, §3]).

ACKNOWLEDGEMENTS

The author is supported by NSF award DMS-1402268. He thanks Pete L. Clark for helpful discussions about arithmetic in $\text{Prin}(\mathbf{Z}_K)$, and he thanks Carl Pomerance for suggesting the consideration of the behavior of the $\text{Prin}(\mathbf{Z}_K)$ divisor function.

REFERENCES

- [Add57] A.W. Addison, *A note on the compositeness of numbers*, Proc. Amer. Math. Soc. **8** (1957), 151–154.
- [BÖRS05] D.M. Bradley, A.E. Özlük, R.A. Rozario, and C. Snyder, *The distribution of the irreducibles in an algebraic number field*, J. Aust. Math. Soc. **79** (2005), 369–390.
- [EK40] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742.
- [Ell80] P.D.T.A. Elliott, *Probabilistic number theory II: Central limit theorems*, Grundlehren der Mathematischen Wissenschaften, vol. 240, Springer-Verlag, Berlin-New York, 1980.
- [GHK06] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [GR09] A. Geroldinger and I.Z. Ruzsa, *Combinatorial number theory and additive group theory*, Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser Verlag, Basel, 2009.
- [GS07] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac theorem*, Equidistribution in number theory, an introduction, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, pp. 15–27.
- [Hal68] G. Halász, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hungar. **19** (1968), 365–403.
- [HW08] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.
- [Kac41] M. Kac, *Note on the distribution of values of the arithmetic function $d(m)$* , Bull. Amer. Math. Soc. **47** (1941), 815–817.
- [KL08] W. Kuo and Y.-R. Liu, *The Erdős-Kac theorem and its generalizations*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 209–216.

- [Kro66] J.P.M. de Kroon, *The asymptotic behaviour of additive functions in algebraic number theory*, Compos. Math. **17** (1965-1966), 207–261.
- [Lan99] E. Landau, *Neuer Beweis der Gleichung $\sum_{k=1}^{\infty} \frac{\mu(k)}{k} = 0$* . Dissertation, Berlin, 1899.
- [Lan03] ———, *Über die zahlentheoretische Funktion $\mu(k)$* , Sber. Kais. Akad. Wissensch. Wien **112** (1903), 537–570.
- [Lan11] ———, *Über die Äquivalenz zweier Hauptsätze der analytischen Zahlentheorie*, Sber. Kais. Akad. Wissensch. Wien **120** (1911), 973–988.
- [Lan18] ———, *Über Ideale und Primideale in Idealklassen*, Math. Z. **2** (1918), 52–154.
- [Liu04] Y.-R. Liu, *A generalization of the Erdős-Kac theorem and its applications*, Canad. Math. Bull. **47** (2004), 589–606.
- [LR01] L. Lucht and K. Reifenrath, *Mean-value theorems in arithmetic semigroups*, Acta Math. Hungar. **93** (2001), 27–57.
- [Man97] H. von Mangoldt, *Beweis der Gleichung $\sum_{k=1}^{\infty} \frac{\mu(k)}{k} = 0$* , Sber. Kgl. Preuß. Akad. Wiss. Berlin (1897), 835–852.
- [Nar86] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Mathematics, vol. 1087, Springer-Verlag, Berlin, 1984.
- [Nar04] ———, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.
- [Ols69] J.E. Olson, *A combinatorial problem on finite Abelian groups. I*, J. Number Theory **1** (1969), 8–10.
- [Pil40] S.S. Pillai, *Generalisation of a theorem of Mangoldt*, Proc. Indian Acad. Sci., Sect. A. **11** (1940), 13–20.
- [Rém66] P. Rémond, *Étude asymptotique de certaines partitions dans certains semi-groupes*, Ann. Sci. École Norm. Sup. (3) **83** (1966), 343–410.
- [Sel39] S. Selberg, *Zur Theorie der quadratfreien Zahlen*, Math. Z. **44** (1939), 306–318.
- [Web96] H. Weber, *Ueber einen in der Zahlentheorie angewandten Satz der Integralrechnung*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1896), 275–281.

UNIVERSITY OF GEORGIA, DEPARTMENT OF MATHEMATICS, ATHENS, GEORGIA 30602, USA
E-mail address: pollack@uga.edu